

it-sa 2023

SECURE IDENTITIES FOR IIOT AND IOT

BXC
CONSULTING

FOR IMPACTING 
BUSINESS SOLUTIONS

SECURE IDENTITIES AND CREDENTIALS

Secure Authentication is the starting point for an effective Access Control system



IDENTITIES

- The standard IEEE 802.1AR – Secure Device Identity defines cryptographically protected identities for devices as requirement for secure identities
- Unique identifier must be specified for the environment, where a device shall be used
- For IIoT devices, supplier identifiers must be translated into operators' identifiers following a defined naming scheme
- Mechanisms to validate identities in the environment must be available to allow trust establishment during communication



CREDENTIALS

- RFC 5280 is the standard for X.509 certificates, supported in the industry by a wide range of devices and applications
- Through flexible certificate structure, various attributes possible to reflect identity in different formats, if possible (e.g., hostname, serial number)
- Certificate-based authentication is the de-facto standard in the industry for mutual machine-to-machine authentication
- Many IoT and OT devices and services support digital certificates for mutual authentication in IP networks

PKI offers widely supported and standards-based digital identities and authentication processes for a variety of devices and services

IMPORTANT STANDARDS

To cover the topic sustainably, some important standards in that field should be considered

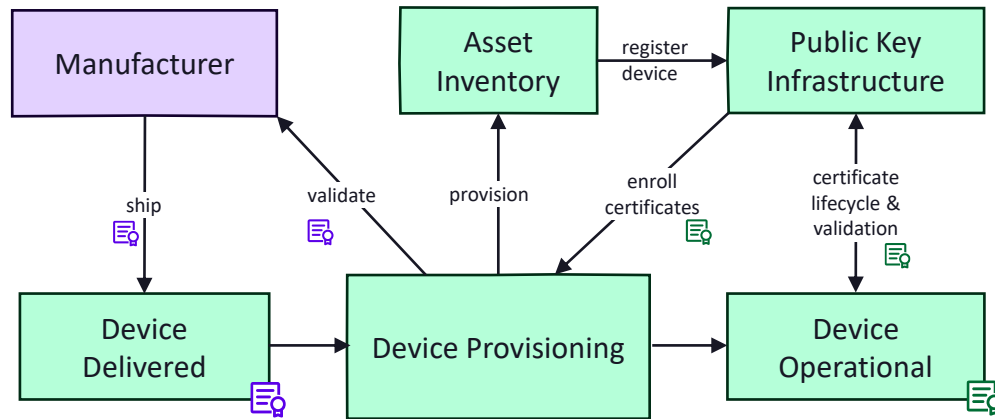
Service	OPC UA	MQTT	REST	Interoperability for vendor-independent data exchange
Network	PROFINET	Wi-Fi	Thread	Secure authentication and network traffic encryption of communication peers
Provisioning	RFC 8995	MATTER		Secure and automated bootstrapping of devices into an operational environment
Identity	IEEE 802.1AR			Standard for Secure Device Identities that defines relationship and requirements for supplier-generated and operator-managed identities
Credentials	RFC 5280			X.509 certificates – cryptographically secured identity tokens

IIoT

IoT

AUTOMATED PROVISIONING






Handling device onboarding in an automated way reduces manual effort for OT Engineers and provides high level of confidence for registered device information in Asset Inventory as central Device Identity Management system

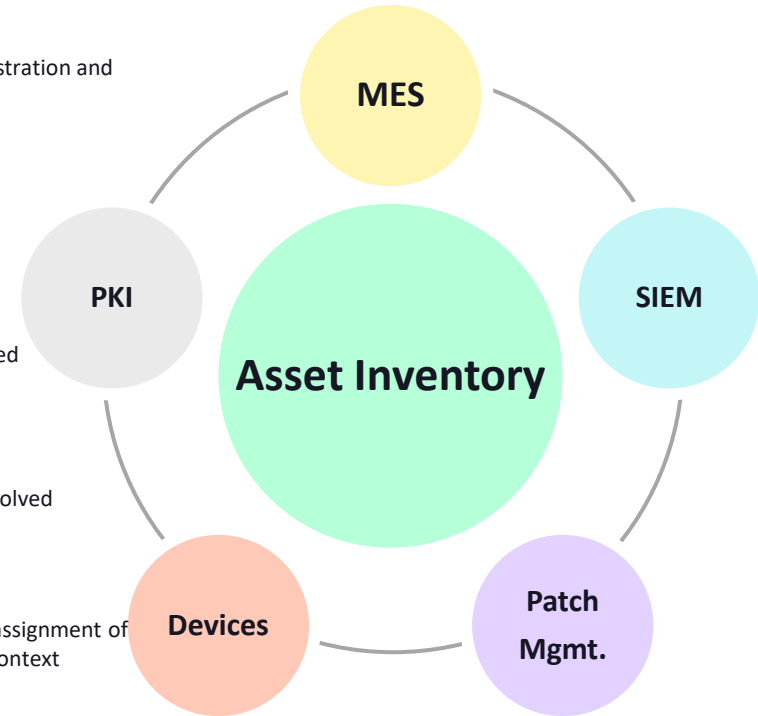


- Secure onboarding of devices into operations can be highly automated with BRSKI (IEEE 802.1AR)
- IDevID is used to validate authenticity of delivered device
- Provisioning of LDevID and organizational certificates can be automated with various PKI enrollment protocols e.g., EST, CMP
- Manual effort for operations significantly reduced for onboarding of new devices into the environment

ASSET INVENTORY

The Asset Inventory of the organization should be developed as central lifecycle management service for all devices to increase automation of processes and security controls

-  MES can leverage additional device information for manufacturing process orchestration and planning and enrich information
-  Device identity information provides valuable context and environmental information for security monitoring services
-  Central management of identified vulnerabilities and patch status allows risk-based application of cybersecurity controls
-  Processes for the lifecycle management of devices can be centrally used by all involved organization entities
-  The inventory acts as central identity database for devices and allows automatic assignment of certificate templates and enrollment processes depending on device status and context



PLEASE REFER TO

WWW.BXC-CONSULTING.COM

FOR FURTHER DETAILS AND
INSIGHTS ON BXC.

FIND US AT IT-SA

BUILDING 7 – BOOTH 239

FOR INTERESTING TALKS